



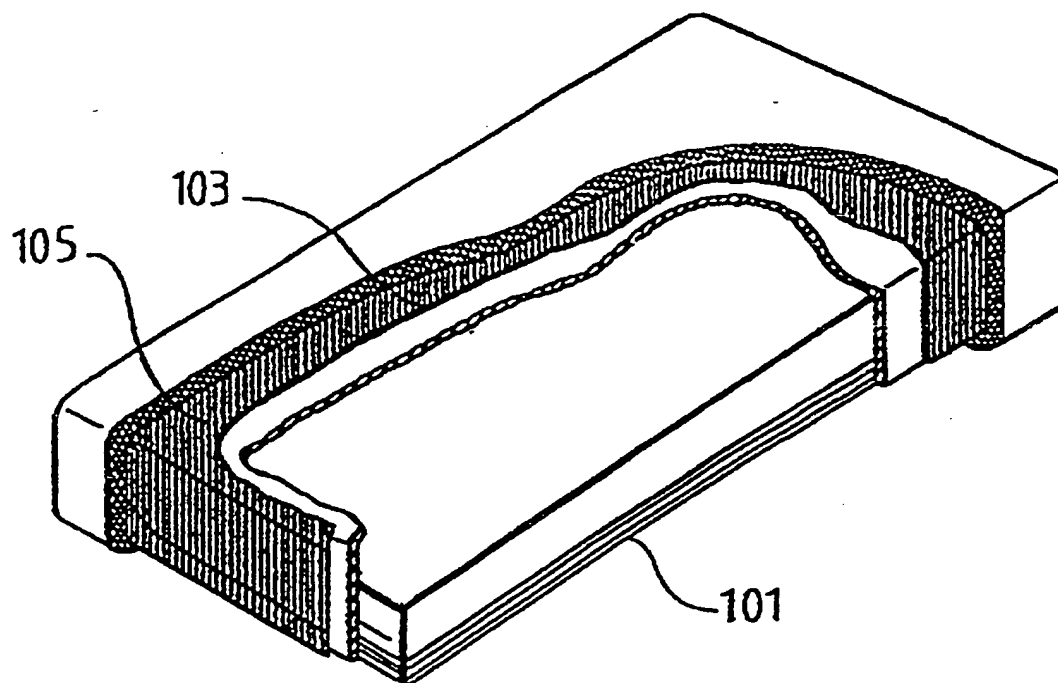
US 20010056542A1

(19) **United States**(12) **Patent Application Publication** (10) Pub. No.: **US 2001/0056542 A1**
Cesana et al. (43) Pub. Date: **Dec. 27, 2001**(54) **TAMPER RESISTANT CARD ENCLOSURE
WITH IMPROVED INTRUSION DETECTION
CIRCUIT**(30) **Foreign Application Priority Data**

May 11, 2000 (GB)..... 0011247.4

Publication Classification(75) Inventors: **Mario Leonardo Cesana, Besana
Brianza (IT); Roberto Antonio Zavatti,
Milan (IT)**(51) Int. Cl.⁷ **H01L 23/552**(52) U.S. Cl. **713/194; 257/902****Correspondence Address:****IBM Corp, IP Law, N50/040-4
1701 North Street
Endicott, NY 13760 (US)**(73) Assignee: **International Business Machines Cor-
poration, Armonk, NY**(21) Appl. No.: **09/850,917**(22) Filed: **May 7, 2001**(57) **ABSTRACT**

A system for protecting an electronic device from mechanical intrusion attempt. An intrusion barrier able to detect mechanical intrusion by means of circuit traces which detect any change in the resistance characteristics of the electric circuit. These circuit traces function as a resistors and they are connected together to form a Wheatstone bridge. According to the present invention the logical lay-out of these connections is selected so that the voltage difference between two adjacent traces is minimized. In this way the current leakage effect is limited to the minimum.



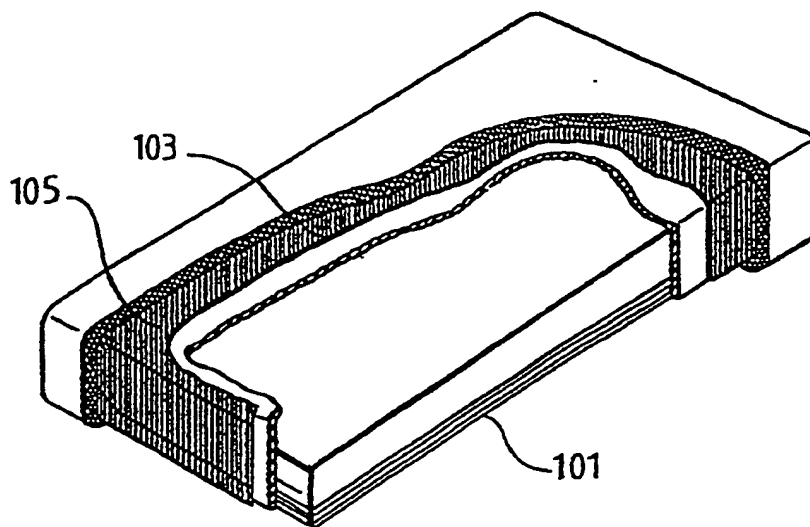


FIG. 1

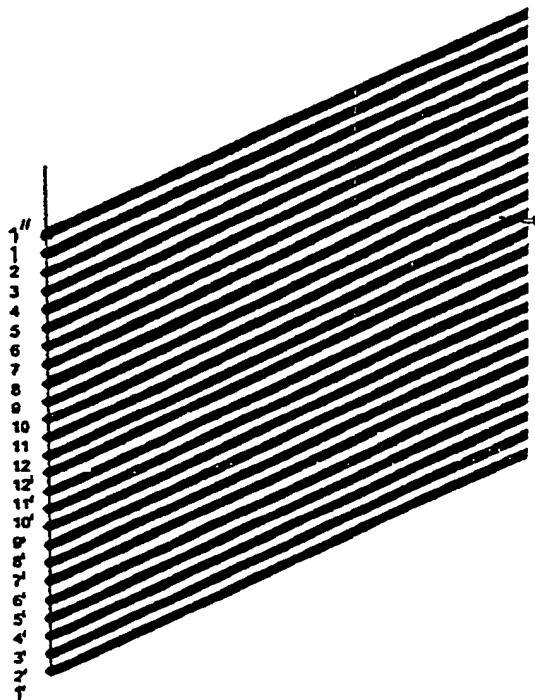


FIG. 2

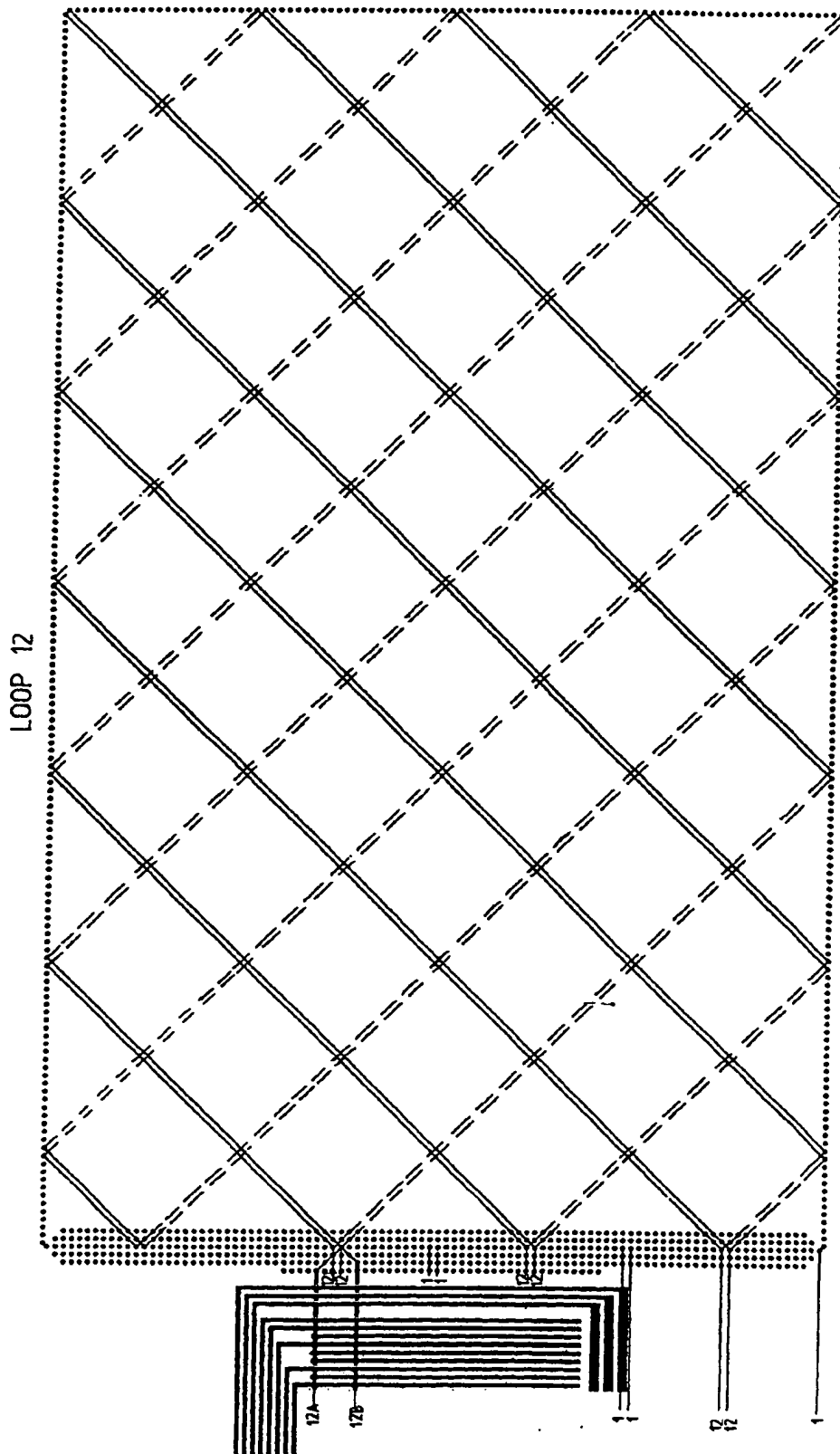


FIG. 3

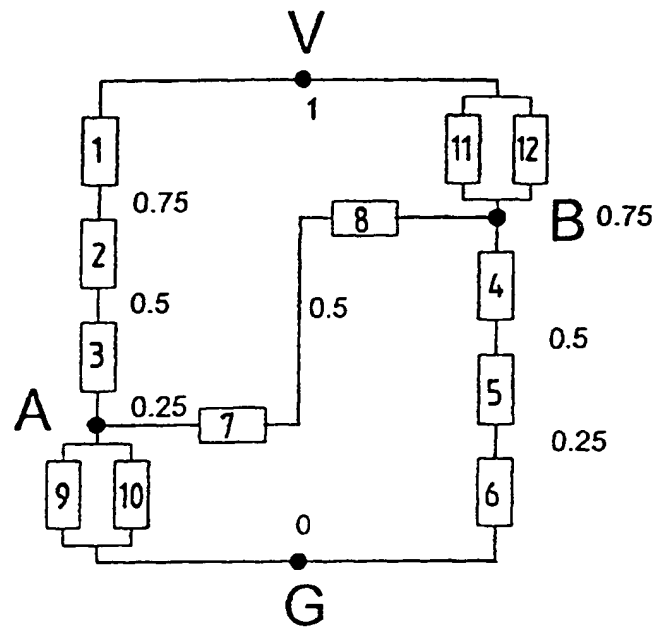


FIG. 4

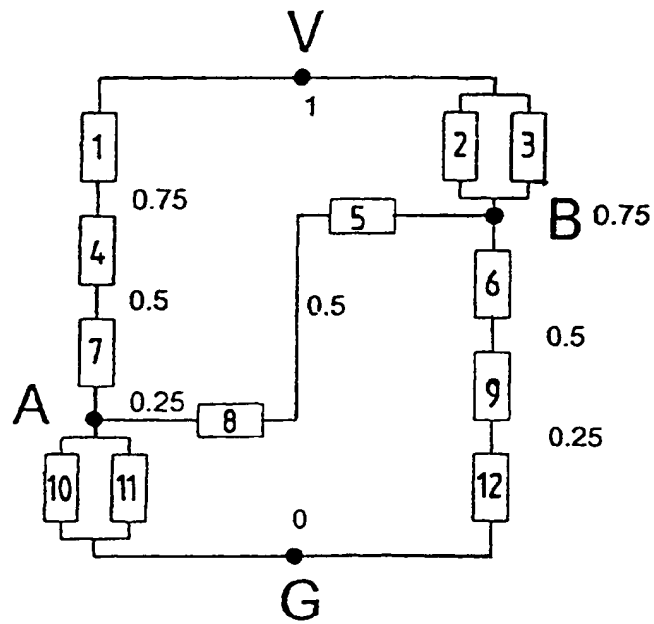


FIG. 5

TAMPER RESISTANT CARD ENCLOSURE WITH IMPROVED INTRUSION DETECTION CIRCUIT

FIELD OF INVENTION

[0001] The present invention relates to protection of electronic cards from unauthorised intrusion, more particularly the present invention relates to a security enclosure with an improved intrusion detection circuit.

BACKGROUND OF THE INVENTION

[0002] It is a usual requirement for many computer applications to protect data from unwanted access by an unauthorised user. Many software protection systems are known in the art to allow only selected users to access said protected data, with the use of a password or other identification methods. Communication of data on a network is protected from undesired detection by means of encryption methods. Passwords, encryption keys and other sensitive data are usually stored in memory components in the computer systems and need to be protected even more carefully from unwanted inspection. Software control and protection methods may be not enough to stop an experienced person from bypassing these protections and tampering with the computer hardware, e.g. by direct interrogation of memory components such as integrated circuit memory.

[0003] A possible protection from the above physical attacks is to provide some kind of detecting means which detects an attempted intrusion within a protected sensitive area and reacts by giving an alarm or even by destroying any sensitive information to avoid the loss of secrecy.

[0004] U.S. Pat. No. 5,027,397 describes an intrusion barrier for protecting against mechanical and chemical intrusion into an electronic assembly. The barrier includes a screen material surrounding the electronic assembly. The screen material has formed thereon fine conductive lines in close proximity to each other in a pattern that limits the mechanical access which could be achieved without disturbing the resistive characteristic of at least one line or line segment. The lines are formed of conductive particles of material dispersed in a solidified matrix of material which loses its mechanical integrity when removed from the screen substrate. Electrical supply and signal detection means are provided which are adapted to supply a signal to the conductive lines and generate an output signal responsive to a given change in the resistance of the conductive lines whereby, when the resistance of the conductive lines changes, either as result of chemical or mechanical attack, a signal is generated which causes an alarm and the erasure of sensitive information in the protected memory component.

[0005] In order to better protect the content of the security enclosure from the most sophisticated intrusion techniques, the wires should also be invisible and not detectable. For this reason it is known to make these wires with non-metallic, x-ray transparent, (low) conductive materials, merged into a resin having color, physical and mechanical characteristics very similar to the conductive tracks. This requirement constitutes a significant constraint in the choice of the material for the resin which often provides poor electrical insulation. In some circumstances the insulation deteriorates with the increase of the temperature and this makes the detecting circuit unstable and prone to false tamper detection. This problem is due to the current leakage through the resin.

[0006] It is an object of the present invention to alleviate the above drawbacks of the prior art.

DISCLOSURE OF THE INVENTION

[0007] According to the present invention, we provide a tamper resistant enclosure for protecting an electronic device comprising an intrusion detection barrier with a plurality of circuit traces for detecting mechanical intrusion attempts which cause a change in the resistance of said circuit traces, the circuit traces being connected according to a logical layout, the logical layout of the circuit traces being selected so that, in use, the voltage differences between adjacent circuit traces are minimized.

[0008] Also according to the present invention we provide an assembly including an electronic device needing protection from unauthorised intrusion, and a tamper resistant enclosure as described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Various embodiments of the invention will now be described in detail by way of examples, with reference to accompanying figures, where:

[0010] FIG. 1 shows schematically a tamper resistant card enclosure according to a preferred embodiment of the present invention.

[0011] FIG. 2 and 3 show a physical layout according to a preferred embodiment of the present invention;

[0012] FIG. 4 shows the connection of the circuit traces by means of a Wheatstone bridge according to the prior art;

[0013] FIG. 5 shows the connection of the traces by means of a Wheatstone bridge according to a preferred embodiment of the prior art.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] With reference to FIG. 1 a tamper proof enclosure according to a preferred embodiment of the present invention is shown. The enclosure is compliant to F.I.P.S. (Federal Information Protection Standard) 140-1 Level 4. An electronic device 101 containing sensitive information (e.g. an electronic cryptographic device), is protected by an intrusion barrier 103. As explained above with reference to prior art (U.S. Pat. No. 5,027,397) the intrusion barrier 103 includes circuit traces 105 which are able to detect mechanical intrusion. When a change in the resistance of the circuit traces is detected, the system assumes that a tampering is being attempted and it reacts by giving an alarm and by erasing all the sensitive information contained in the protected electronic device 101. According to a preferred embodiment of the present invention, the intrusion barrier 103 is a flexible tape e.g. as the one described in U.S. Pat. No. 5,285,734. This flexible tamper respondent sheet preferably has a delamination respondent layer and a laser and pierce respondent layer which includes tracks of electrically responsive material. The tracks are monitored, so that an attempt to penetrate the layer results in one or more of the tracks being cut to produce a detectable change in a monitored electrical characteristic of the tracks.

[0015] According to a preferred embodiment of the present invention each wire has the same resistance value.

The wires act as resistors connected together: when one of these wires (circuit traces) is interrupted the resistance value of the circuit changes and a tamper attempt is detected.

[0016] According to a preferred embodiment of the present invention, the mesh corresponding to the example of FIG. 1 is a continuous pattern of e.g. 12 wires running in parallel all around the enclosure. The mesh is laid out on two layers, and only one (top) is in contact with the resin. The layout of the top layer is represented in FIG. 2. The 12 wires have 12 adjacent start points. The 12 wires run in parallel and after a complete loop they restart in a mirrored sequence adjacent to the start points (numbers from 1' to 12'). FIG. 4 shows the complete route of one of the 12 wires (loop 12) of the example above. It starts at point 12a and arrives after many crossings at point 12b. In FIG. 4 the continuous lines indicate the wires on the top side of the flexible tape; when they arrive on the border they pass on the other side and continue the route; the dotted lines indicate the wires on the bottom side.

[0017] The terminals of the wires are then connected together to form a circuit, which is able to detect an intrusion attempt by monitoring the resistance value. The connection is realised by means of a connection matrix as also described in U.S. Pat. Nos. 5,539,379 and 5,285,734. As mentioned above the wires act as resistors in this circuit. It is usual to connect them together to form a Wheatstone bridge as the one represented in FIG. 4. A Wheatstone bridge has a minimum of 4 (or 5 if there is a central one) resistors, but each one may be split in two or more resistors.

[0018] According to a preferred embodiment of the present invention, a Wheatstone bridge having 12 resistors (wires) has been used to create the circuit traces for intrusion detection barrier as represented in FIG. 5. It is a logical diagram where each wire has the same length and is represented in FIG. 5 by a resistor. A voltage V_b is applied between terminals V and G, while terminals A and B are monitored. Under normal conditions, A will measure $0.75 \times V_b$, B will measure $0.25 \times V_b$. In case one or more wires are interrupted or shorted, the voltage at terminals A and B will trip and the electronic circuit connected to the mesh will detect a tamper.

[0019] As mentioned above, the resin is not an ideal insulator; for this reason an electrical path can be established between two adjacent wires. This results into an apparent decrease of resistance of the branches in the circuit and possibly in a measurable voltage trip at terminals A and B. This can cause a false tamper detection.

[0020] This phenomenon is called current leakage; it has been discovered that it depends on several factors:

[0021] the distance between tracks;

[0022] the resistivity of the resin;

[0023] the length of wires;

[0024] the voltage difference between two adjacent wires.

[0025] The first three parameters are very difficult to modify either for performance reasons (e.g. the distance between tracks should be as short as possible) or for design requirements (e.g. the size of the package).

[0026] According to the present invention the current leakage problem is minimized by reducing as much as possible the voltage differences between each couple of adjacent wires. According to a preferred embodiment of the present invention, this is achieved by choosing an appropriate logical layout of the wires (i.e. the connection among the wires), based on the observation that at each terminal of the 12 resistors the voltage applied is the one indicated in FIG. 5.

[0027] In fact four groups of 3 resistors (wires) each can be identified where the resistors have the same voltage.

[0028] Table 1 shows the solution which minimizes the voltage difference between adjacent wires for the example shown above, assuming the current flows in the same direction on all wires.

TABLE 1

Voltage difference ($\times V_b$)	between wire	and wire
<0.25	1"	1
0	1	2
0	2	3
0.25	3	4
0	4	5
0	5	6
0.25	6	7
0	7	8
0	8	9
0.25	9	10
0	10	11
0	11	12
<0.25	12	12'

[0029] FIG. 6 shows a possible layout for the example above according to a preferred embodiment of the present invention. With respect to the prior art it can be seen that no adjacent wires differ in voltage by more than $V_b/4$. Each of the above mentioned group of three resistors (i.e. wires) are made by adjacent wires (e.g. 1, 2 and 3; 4, 5 and 6). Only between 3 and 4, 6 and 7 and so on there is a voltage difference, which is limited to $V_b/4$. In general, the voltage difference between adjacent lines is thus minimized, reducing the risk of current leakage described above. Those skilled in the art will appreciate that other layouts can be used instead of the example above with different number of wires.

What is claimed is:

1. A tamper resistant enclosure for protecting an electronic device comprising an intrusion detection barrier with a plurality of circuit traces for detecting mechanical intrusion attempts which cause a change in the resistance of said circuit traces, the circuit traces being connected according to a logical layout, the logical layout of the circuit traces being selected so that, in use, the voltage differences between adjacent circuit traces are minimized.

2. The tamper resistant enclosure of claim 1 wherein the logical layout comprises a network of said traces connectable between two reference voltages, said traces, in use, dividing said network into a series of potential drops, each trace occupying a place in said series no further than one potential drop from an adjacent trace.

3. The tamper resistant enclosure of claim 2 wherein the logical layout is a Wheatstone bridge.

4. The tamper resistant enclosure of claim 3 wherein the Wheatstone bridge comprises a number N of resistors, N being a multiple of 12.

5. The tamper resistant enclosure of claim 4 including three series of potential drops, each comprising $N/3$ traces, each potential drop being equal to $3/N$ of the difference between the reference voltages.

6. The tamper resistant enclosure of claim 1 wherein the circuitized intrusion barrier is a flexible tape.

7. An assembly including an electronic device needing protection from unauthorised intrusion, and the tamper resistant enclosure of claim 1.

* * * * *